

LEGISLATIVE AUDIT DIVISION

Scott A. Seacat, Legislative Auditor
John W. Northey, Legal Counsel



Deputy Legislative Auditors:
Jim Pellegrini, Performance Audit
Tori Hunthausen, IS Audit & Operations
James Gillett, Financial-Compliance Audit

MEMORANDUM

DATE: June 8, 2004

TO: Legislative Audit Committee Members

FROM: David Nowacki
Information Systems (IS) Auditor

RE: Montana State University (MSU) Key Application and General Controls
IS Audit - 04DP04

INTRODUCTION and BACKGROUND

Montana State University (MSU) uses Banner, a mature commercial software application, to manage its business processes. In addition to student data MSU uses Banner to process student financial aid, human resource, and financial information. Because data from all four MSU campuses resides on servers located at the Bozeman campus, MSU – Bozeman's Information Technology Center (ITC) is responsible for Banner information technology (IT) environment administration and security. Additionally, ITC is the central administrative body for the MSU – Bozeman campus network and IT facilities, and provides guidelines and requirements for department IT administrators.

AUDIT SCOPE

The audit scope was conducted in accordance with Government Auditing Standards published by the U.S. General Accounting Office. We evaluated the control environment using information security best practices, control objectives for information technology COBIT®, SANS Institute, Security Checklist for Oracle 9i, and Board of Regents Policy.

We audit select MSU Banner processes approximately every two years to understand the control environment. The prior MSU Banner Information Systems (IS) Audit (01DP-05) was issued May 2001 and subsequent support work (03DP-06) performed testing and updated specific controls. The current audit scope is based on specific control testing requested by financial compliance staff and specific general controls testing determined relevant to the Banner application.

Data from all four MSU campuses is stored centrally on servers located on the Bozeman campus; therefore, general controls fieldwork was performed exclusively for the MSU – Bozeman campus. Back-up and fail-over facilities are located on the MSU – Billings campus, but were not included in this audit scope.

AUDIT OBJECTIVES and METHODOLOGY

Application Controls

Application controls work was performed to provide assurance on specific controls identified by financial compliance audit staff. A technical memorandum has been provided to financial compliance staff communicating the existence and operation of Banner application controls.

We reviewed application controls over the finance, student financial aid, and human resources modules in Banner. We ensured the payroll deduction rates and leave accrual rates residing in the underlying system tables contained appropriate rates consistent with the current year governing federal or state law, and the activity date is consistent with the applicable rate effective date. For specific automated student financial aid forms, we determined procedures are in place to limit system access and input functions to current employees. We reviewed the download process from the Department of Education to ensure the information exchange is complete and the upload process to the student aid module is controlled. We determined that the cost of attendance amounts residing in Banner are consistent with the rates developed by the Financial Aid Office for the most current academic year. We also determined the way Banner handles satisfactory academic progress policy operates according to management assertions. Access to automated forms used to reduce or adjust student accounts receivables was limited to appropriate individuals currently employed by MSU.

General Controls

The primary objective was to provide reasonable assurance that controls exist over the Banner system software, hardware, and data to ensure they are protected from unauthorized or unnecessary access, and environmental threats. We tested specific general controls identified as relevant to the Banner application.

- 1. Physical access controls protect Banner devices from unintentional or malicious harm, and environmental controls protect Banner system assets from known and probable events.**

Objective was accomplished through observing the facilities housing critical Banner equipment, and interview with MSU Bozeman staff. We conclude that the physical security environment at the time of our observations is adequate to prevent and detect unauthorized access, protect against fire, excessive temperatures, flooding, power loss, and backup data.

- 2. Windows operating system is configured to prevent unauthorized access and protect against commonly known exploits.**

Using a combination of network audit tools, we tested servers directly related to Banner operations on the Bozeman campus for missing patches and potentially unnecessary services running. We conclude that Banner servers were properly patched and running only necessary services. Additional testing was done on select departmental servers that could potentially access Banner. During our work specific servers were identified which attracted our concern; we requested ITC follow up on these concerns. A management memorandum was transmitted to MSU addressing these additional servers that warrant management attention, but do not require further disclosure in this report. Subsequent to our work, a Campus Networking Policy was adopted May 2004. We will follow up on policy implementation and enforcement during the next MSU audit.

3. UNIX users, user groups and access are controlled.

To verify controlled access, we reviewed the UNIX group and password configuration. We conclude that all active non-system users are current MSU employees, user passwords are shadowed and encrypted or disabled from logging in, there are no guest accounts, no ordinary users have access to the root directories, and password shadowing is used for groups.

4. Oracle delivered default users' passwords are changed upon installation, or locked.

We checked for unchanged passwords related to default Oracle user accounts. We conclude that default passwords were changed for all Oracle default accounts.

5. Oracle system access privileges are controlled.

We reviewed a query of users that have been granted Oracle delivered roles and administrative roles, and whether users had the ability to grant permissions to others. Based on testing performed, Oracle system access is controlled by only granting administrative roles to individual users as necessary.

6. MSU Banner Security Planning Process is in place.

Through interview with associate directors for the Administrative Systems and the Network, Systems, and Operations, and MSU Executive Director for IS and Chief Information Officer, we obtained policies and procedures for discussion. Of significance to the Security Planning Process were:

- MSU Security Plan for Information Technology (IT) Systems, January 2004
- Computer Security Incident Handling Procedure
- MSU Security Management Team Charter & Objectives, March 30, 2004
- Standards for Network Connectivity
- MSU Report on the Implementation of IT Policies, Submitted to MT Board of Regents
- Campus Networking Policy
- System Security
- Risk Matrix Diagrams

The MSU Security Plan for IT, January 2004 is in template form; our review of the above documentation determined that fundamental issues and structure, policy and procedures of each address security issues.

When discussed with MSU management, we conclude that a Security Management Team exists that is responsible for developing and promoting sound security practices, and a documented commitment from MSU has been made to delegate the responsibility of drafting, establishing and implementing a plan, review by Internal Audit, review by campus groups and advisory committees within 90 days, and formally adopted by August 13, 2004.

7. MSU has processes in place to ensure IT services are available and there is minimum impact caused by disrupting events.

We obtained the most recent Business Continuity Recovery Plan and discussed with MSU management. We conclude that responsibilities have been delegated to specific job roles, and backups specified in the event of a disaster. Procedures are specified throughout the plan.

MSU recognizes that they need to be more diligent in quarterly testing of disaster fail-over services, and conduct an annual review of the Disaster Recovery and Business Continuity Plan.

CONCLUSION

We conclude that application controls specifically identified by financial compliance operate to ensure that payroll and leave accrual rates are timely and accurate, student financial aid input and access functions are limited to active MSU employees, student aid information is completely downloaded from the U.S. Department of Education and completely uploaded to Banner, cost of attendance amounts are accurate, satisfactory academic progress operates according to management assertions, and student accounts receivable access and input functions are limited to active MSU employees.

Additionally, we conclude that adequate controls exist over the general controls environment to ensure that Banner system software, hardware, and data are protected from unauthorized or unnecessary access and environmental threats.

S:\ADMIN\IS\BANNER\MSU\dn.June LAC.memo.doc/bb